For example, when a Web browser points to a secured domain, a Secure Sockets Layer handshake authenticates the server (Web site) and the client (Web browser). An encryption method is established with a unique session key

Every SSL Certificate is created for a particular server in a specific domain for a verified business entity. The SSL Certificate is issued by a trusted authority, the Certificate Authority. When the SSL handshake occurs, the browser requires authentication from the server. A customer sees the organization name when they click certain SSL trust marks or use a browser that supports Extended Validation. If the information does not match or the certificate has expired, the browser displays an error message or warning.

The description of how the invention functions supports the use of the "split key language as there is a public and private key described.

The Examiner is respectfully requested to reconsider his rejection of claims 1 - 4, 10 and 11 under 35 U.S.C. §102(e) as being anticipated by United States Patent 5,933,785 to Tayloe.

The Examiner is respectfully requested to review his interpretation of the Tayloe reference and the manner in which he has applied same to the claims in the instant application. By virtue of the nature of the rejection under 35 U.S.C. $ 102(e), the Examiner is asserting that each and every element claimed by Applicants is found in the Tayloe reference. The Examiner in his rejections in the above-noted Office Action cites the specific language found in Applicants' claims and bases his anticipation rejections on excerpts which, in fact, do not support his assertions and are taken out of context.

The Examiner's rejections are quoted ***verbatim*** and listed ***seriatem,*** with Applicants' responses to the specific rejection presented immediately thereafter.

The Examiner says: "As to claim 1, Tayloe discloses a method for setting basic means of access for operation of devices of which the operation is controllable by electronic means, comprising: the devices comprising mobile phones, small computer-controlled consumer devices with relatively low level of computing power, computers, motor vehicles, control terminals for industrial processes, all of which devices may require authentication prior to operation [Column 2, line 59 to Column 3, lines 27 - 34]..."

Response: Applicants respectfully submit that Tayloe does not disclose the variety of devices that are claimed by Applicants. In only referring to cellular phones or personal communication devices. There is no mention of the other devices. Tayloe discloses at Column 2, line 59 to Column 3, lines 27 – 34:

"Upon power-up of the radiotelephone 101, a SIM card 105 is inserted by the user into the SIM card reader 107 contained within the radiotelephone 101. Upon insertion of the SIM card 105, the radiotelephone 101, prompts the user through the user interface 109 to insert a personal identification number (PIN) to unlock the SIM card allowing access to the subscriber information contained therein. In other embodiments, the SIM card may not require the entry of a PIN number to unlock the subscriber information contained therein. Upon entering the SIM card access PIN, the radiotelephone 103 executes the process 300 illustrated in FIG. 3 and subsequently described in detail. After successfully completing the process 200, a radiotelephone 101 is fully registered for service in the radiotelephone system 100 of FIG. 1. The radiotelephone 101 is now able to send and receive RF signals from the remote transceiver 101."

In reviewing this cited text, there is no mention of the other devices claimed, and there is no teaching nor suggestion that the RF signals are used for any purpose other than operation of the radio telephone. A reading of the entire specification confirms that the Tayloe invention is restricted to implementing the use of universal identification numbers or telephone numbers and to permit a single number to be used on different networks. Consequently there is no proper basis upon which to expand the teaching.

Tayloe discloses a communication system that uses Subscriber Identity Module. This system differs from the present invention in its use of the Subscriber Identity Module. While this module is a "Smart Card" its is different from the Smart Card used in accordance with Applicants' invention.

A Subscriber Identity Module (SIM) is a removable smart card. Its function is to securely store the key identifying a mobile phone service subscriber. The SIM card allows users to change phones easily by removing the SIM card and inserting it into another mobile phone, thereby eliminating the need for activation of the new mobile phone on the network. The use of SIM card is mandatory in the GSM world.

SIM cards store network specific information used to authenticate and identify subscribers on the Network. Each SIM is internationally identified by its ICCID (International Circuit Card ID). ICCIDs are stored in the SIM cards and are also engraved or printed on the SIM card body during a process called personalization.

SIM cards are identified on their individual operator networks by holding a unique International Mobile Subscriber Identity. Mobile operators connect mobile phone calls and communicate with their market SIM cards using their IMSI.

SIM stores network state information, broadcasted to it from the network, such as the Location Area Identity (LAI). Operators networks are divided into Location Areas, each having a unique LAI number. When the Mobile changes its location from one Location Area to another it stores its new LAI in SIM and sends it to the operator network to inform network with its new location. If the handset is turned off and back on again it will take data off the SIM and search for the LAI it was in. This saves time by avoiding having to search the whole list of frequencies that the telephone normally would.

The inherent manner in which the SIM operates renders it unsuitable for considering same in accordance with the present invention.

Applicants have covered the use of a password such as is the means for security described by Tayloe in the specification on Page 2, lines 12 – 25. The present invention is an improvement over that system as described by Tayloe.

The present invention is used by a particular software application on the system to verify access authorization. This could be a single software application, which evaluates the security token and is running on top of the used hardware. Applicants detail the usage of the token to provide specific configuration information, which defines constraints for the usage of a particular user. This "constraint" e.g. temporary deactivation, limits the usage of a reduced feature set. This is more than just "authentication". It adds "authorization" patterns. The support for this is disclosure is found at page 15, the last full paragraph:

"A company telephone system consists of 20 telephones hierarchically grouped into three levels, with corresponding scopes of functions. The telephone sets themselves are produced uniformly and are assigned their actual features only by means of the configuration procedure, which enables or disables various logic components in the sets depending on the customer's specific requirements."

The rejection continues:

"...the authentication comprising temporary deactivation which adds authorization patterns prior to operation [Column 6, lines 27 - 34.

Response:

Column 6, lines 27 – 34 of Tayloe states:

"...When a number is deactivated step 310 deregisters the user with the network it was connected to. This would normally occur when the SIM is withdrawn from the phone, but may happen according to a scheduled event (turn off a number at a scheduled time) or alternatively may be manually invoked (user no longer wants to receive calls on that number)."

The "deactivation step referred to by Tayloe is one that involves the use of the phone when the operator is finished using the phone. Applicants are deactivating the system to add authorization patterns prior to operation. (Emphasis added).

The rejection continues:

"establishment of a link between a personal authentication system supplied with encryption data and a logic system able to control an electronic device control, the encryption being stored solely in the authentication system, the link between the authentication system and the device being via wired of wireless means [Column 3. lines 39-49].

Response: Applicants are not sure of the relevance of the cited excerpt with respect to the instant invention. Tayloe states at Column 3, lines 39 - 49:

"In accordance with the principles of the invention a communications device 101 is provided with the capability to accept a SIM card 105 having multiple universal numbers, each with its own user specific encryption algorithms. The communication device 101 is therefore able to provide service for more than one user and in particular, to be able to accept incoming calls. For each different universal identification number, the device 101 can keep track of the encryption necessary for each number and, if necessary, register that number on the system currently providing service."

There is no reference in the excerpt cited that anticipates the element of the claim cited by the Examiner. Tayloe is setting up a connection between the SIM and the cellular phone, but he is using a completely different security system to do so. It is essential to note in properly evaluating the overall system disclosed by Tayloe that the algorithm has to be stored on the SIM (Column **3,** lines 40 -42), Applicants' Claim 1 distinguishes their invention from Tayloe by reciting that: ***"said encryption data being stored solely in said authentication system."*** In the event a public or private key infrastructure is used, the required keys are stored in their entirety; for example, on the smart card as well as on the device. This is not the case for the SIM. In Applicants' invention, a key may be present on the device and the same key on the smart card, so a

challenge/response can be used to authenticate the smart card. Further Applicants positively recite that they use a ***"non-split key*** " in the claims.

The rejection continues:

"checking the encryption data in the authentication system prior to operation of the electronic device control [column 3 lines 39-49];

It appears in Tayloe that the user is granted access to the contents of the SIM including its networked resources. One must infer, because there is no definitive disclosure in the reference, that there is only one level of authentication (access yes/no). Please note that the credentials are loaded from the user onto the SIM. In Applicants' invention, there is no need to transfer the credentials to the host. In particular it is preferable to keep the credentials on the smart card.

The rejection continues:

"assignment of a plurality of predetermined means of access to the electronic device control associated with the authentication system the predetermined means providing access to the physical hardware resources and access to different software functions, based on the privileges of the user who identified himself to the system, the software function evaluates a security token and is running on top of the physical hardware [Column 2, lines 59 to Column 3, line 7]"

Response: In the Tayloe patent, when considering ***"access,"*** there is only a single level of access. An important distinguishing key to the present invention is that there are different levels of access to differentiate the different levels of authentication or authorization that persons with different roles may need. The Examiner is referred to page ***6*** of the instant specification. The different levels are mentioned on page 6. At that location, there is a disclosure of the system being open to progressive hierarchies of access rights to the device, for example, by the production of a Master Smartcard which can be issued to customers' service personnel in order to configure large numbers of individual devices.

Further, on page 6: "Applying the method in accordance with the invention, and based on the stipulation that a single SmartCard is to be able to configure any number of devices but ' that only a Master SmartCard or a personal SmartCard can be used to shut down and/or startup/restart the devices, a device manufacturer may do the following..' ."

Applicants have differentiated between a single (standard) smart card (such as the SIM of Tayloe) and a Master Smart Card. The different levels are mentioned in the portion of Claim 1 that reads: "...assignment of a plurality of predetermined means of access to the device associated with the authentication system." Applicants' Claim 1 states: ***"said predetermined means of access being dependent upon the level of authorization that is set in said personal authorization system."***

The final portion of the rejection of Claim 1 states:

"enabling of the means for access predetermined for the authentication system dependent on the result of the check. [Column 2, line 30 to column 3, line 7]."

Response: Applicants cannot locate any teaching or disclosure related to a multi-level security system in Column 2, line 30 to Column 3 line 7, quoted by the Examiner. Tayloe refers to only one level of security. The reference only refers to the manner in which the authentication is performed by using the PIN to unlock the SIM. There is no differentiation based on the role of the user. Claim 1 reads, in pertinent part: "... ***establishment of a non split-key link between a personal authentication system supplied with encryption data and a logic system able to control an electronic device control, said encryption data being stored solely in said authentication system*** ... ·

As to Claim 11, the Examiner has rejected the elements as set forth in Claim 1, and the responses set forth above are incorporated by reference herein for those elements. The Examiner then continues the rejection with the following:

"the method providing means of no access or full access and allow more finely defined levels of access as defined in a user profile for configuration or maintenance work [Column 2, line 59 to Column 3, line 7]."

Response: Applicants cannot locate any teaching or disclosure related to "no access or full access and allow more finely defined levels of access" as defined in a user profile for configuration or maintenance work at the location cited in Tayloe.

Applicants respectfully submit that the rejection of Claim 1 based upon "anticipation" by the Tayloe reference is without proper foundation. The Examiner has misinterpreted the teachings of Tayloe; and based upon this improper interpretation, there is no predicate for the rejection. Each and every element defined in Claim 1 is not found in the Tayloe reference. Thus the rejections of the dependent claims are also improper and incorrect.
The Examiner continues:

"As to claim 2, Tayloe discloses that the basic means of access of functions of the device comprise at least one of the following means: disable operation of the devices, enable operation of the devices, or enable configuration of device. [Column 2, line 59 to Column 3, line 7]."

Response: There is no mention of enabling the basic means of access to functions using the means claims allegedly present at Tayloe, et al. Column 2, line 59 to column 6, line 5. A careful reading of the section reveals that it only refers to access using the SIM card. Thus, there is no anticipation of the elements defined in Claim 2.

The Examiner continues:

"as to claim 3,Tayloe discloses that the link is made without need for intermediate software layers. Column 2, line 59 to Column 3, line 7."

Response: There is no mention that the link is made without the need for an intermediate software layer in Tayloe. The cited location only discusses the "SIM" and NOT how the link is set up.

The Examiner continues:

"As to claim 4, Tayloe discloses in addition, the step of reading at least one of the following features embodied within the authentication system: firmware programs, device-specific command sequences for

execution of specific device-specific functions, cryptographic keys, cryptographic algorithms, and individual decision-making logic. [Column 3, lines 39-49]."

Response: There is no mention of the features claimed in Claim 1. In the excerpt cited by the Examiner, Tayloe only refers to secure transmission or accessing the database that the host contains to store some decrypted data. He notes that there are some encryption alogorithms stored in his unit. Thus, again, there is no anticipation of the elements defined in Claim 4.

The Examiner continues: "As to claim 10, Tayloe discloses program code areas for the execution or preparation for execution of the steps when the program is installed in a computer. [Column 2, line 59 - column 3, line 7."

Response: Applicants can find no relevance in the disclosure at Column 3, lines 39 – 49 relating to the content of Claim 10 and request specific clarification as to the relevance of the cited lines in Tayloe to Claim 10. The excerpt refers to how the SIM is used to get access. The Tayloe disclosure at the cited location has no teaching of installing a computer program on the host.

The Examiner continues: "As to claim 11, Tayloe discloses a means for setting basic means of access for operation of devices of which the operation is controllable by electronic means, comprising: [the balance of the claim is as defined in claim 11.

Response: With respect to responding to the rejection of Claim 11, the responses to each of the elements as set forth above are incorporated by reference herein.

The Examiner is respectfully requested to reconsider his rejection of claims 5 – 9 under 35 U.S.C. §103(a) as being unpatentable over United States Patent 5,933,785 to Tayloe as applied to Claim 1, and further in view of United States Patent 6,415,144 to Findikli, et al.

The rejection under Section 103 is also improper as there is an unwarranted assertion that the elements of Claim 1 are not disclosed by Tayloe. Therefore the rejections of Claims 5 – 9 are improper.

Although the rejection is improper, Applicants will respond to the rejection. The Examiner concedes that Tayloe does not teach that the method disclosed therein that includes

(1) configuration of the devices by authorized persons, and (2) that after successful authentication device specific configuration data are downloaded into the devices from the authentication system in accordance with the authentication system or over a network. With respect to the latter missing element, Applicants reiterate that neither Findikli (nor Tayloe) disclose the variety of devices that are claimed by Applicants. In Column 1, line 61 to Column 2, line 5, which is the supporting basis of a rejection noted above, the reference is only referring to cellular phones or personal communication devices. There is no mention of the other devices. There is no basis upon which to expand the teaching. It is improper to expand the scope of the disclosure to devices other than cellular phones and the like when no positive recitation is found in the art which supports the assertion.

Tayloe essentially relates to a split key system. The Tayloe invention is specifically tailored to operate in a certain manner and is characterized as an improvement over the prior art in which the problems therewith are discussed in Column 1, line 14 to Column 2, line 6. His improvement is a host apparatus which has multiple secure functions which are accessed by a SIM.

Findikli discloses a method of message management using a mobile communications device with a core and protected memories. Findikli, at Column 1, line 6 1 to Column 2, line 5 provides a general description of two over-the-air teleservices with no specific direction of how either of the systems listed is used in conjunction with a specific system. The excerpt cited by the Examiner as being relevant is merely a description of the prior art as known when the application was filed. As to tailoring the cellphones to meet the needs of the subscriber, Findikli states that the systems mentioned would not be effective if the phones had been hard-coded to prevent overwrite. The skilled artisanwould not combine the two references as each is so specific as to be unique in its manner of operation leaving no room for combining with the other. The Examiner cites Findikli saying over-the-air teleservices provide radio telecommunications operators with greater flexibility in tailoring wireless devices to meet the needs of their subscribers. The real task is in the detail of explicating how the "tailoring" is done. There is no basis to extrapolate the cited excerpt to assert that is says any more than what it specifically does disclose.

The Examiner acknowledges that Tayloe does not teach that device specific configuration data are downloaded into the devices from the authentication system etc.

With regard to Claims 5 - 9, Findikli, et al. teach download of configuration information, in an unsecured way. There is no connection to any security system on the device. There is also no way to personalize/customize the configuration without the mobile phone being registered with a service provider, which may not always be the case for all the devices (like to a landline phone, or a washing machine). There is no basis to combine these references.

As to the rejection of Claims 5 - 9, the rejections are improper. The Examiner has only cited the basis for the rejection with respect to the Tayloe reference. The Examiner has not applied the Findikli reference specifically to Claims 5 – 9. He has only provided an excerpt from the disclosure relating to device specific configuration data being downloaded into the devices from the authentication system without explaining in detail the relevance of the disclosure and how it applies in combination to the Tayloe reference.

In order to analyze the propriety of the Examiner's rejections in this case, a review of the pertinent applicable law relating to 35 U.S.C. $-103 is warranted. The Examiner has applied the Tayloe and Findikli, et al. references discussed above using no specificity as to the relevance of how the Findliki reference is relevant and/or is applied to Claims 5 – 9.

The Court of Appeals for the Federal Circuit has set guidelines governing the combination of references.

These guidelines are, as stated are found in Interconnect Planning Corp. v. Feil, 774 F.2d 1 132,1143,227 USPQ, 543,551 :

> When prior art references require selective combination by the court to render obvious a subsequent invention, there must be some reason for the combination other than hindsight gleaned from the invention itself.

A representative case relying upon this rule of law is Uniroyal, Inc. v. Rudkin-Wiley Corn., 837 F.2d 1044,5 USPQ 2d 1434 (Fed. Cir. 1988). The district court in Uniroyal found that a combination of various features fiom a plurality of prior art references suggested the claimed invention of the patent in suit. The Federal Circuit in its decision found that the district court did not show, however, that there was any teaching or suggestion in any of the references, or in the prior art as a whole, that would lead one with ordinary skill in the art to make the combination. The Federal Circuit opined:

> Something in the prior art as a whole must suggest the desirability, and thus the obviousness, of making the combination. [837 F.2d at 1051, 5 USPQ 2d at 1438, citing *Lindemann*, 730 F.2d 1452,221 USPQ 481,488 (Fed. Cir. 1984).]

There is nothing in the references cited which would suggest the desirability of combining the Findikli reference with the Tayloe reference when the specific basis for citing the Findikli reference as to each of the rejected claims has not been covered in the Official Action.

The Examiner in his application of the cited references is improperly picking and choosing. The rejection is a piecemeal construction of the invention. Such piecemeal reconstruction of the prior art patents in light of the instant disclosure is contrary to the requirements of 35 U.S.C. $ 103.

> The ever present question in cases within the ambit of 35 U.S.C. §103 is whether the subject matter as a whole would have been obvious to one of ordinary skill in the art following the teachings of the prior art at the time the invention was made. It is impermissible within the framework of Section 103 to pick and choose from any one reference only so much of it as will support a given position, to the exclusion of other parts necessary to the full appreciation of what such reference fairly suggests to one of ordinary skill in the art. (Emphasis in original) In re Wesslau 147 U.S.P.Q. 391,393 (CCPA 1965)

This holding succinctly summarizes the Examiner's application of references in this case, because the Examiner did in fact pick and choose so much of the Findikli, et al. reference with respect to "device specific configuration data" to support the rejection and did not cover completely or accurately in the Office Action the full scope of what these varied disclosure references fairly suggest to one skilled in the art.

Further, the Federal Circuit has stated that the Patent Office bears the burden of establishing obviousness. It held this burden can only be satisfied by showing some objective teaching in the prior art or that knowledge generally available to one of ordinary skill in the art would lead that individual to combine the relevant teachings of the reference.

> Obviousness is tested by "what the combined teachings of the references would have suggested to those of ordinary skill in the art." In re Keller, 642 F.2d 413,425,208 USPQ 871,881 (CCPA 1981). But it "cannot be established by combining the teachings of the prior art to produce the claimed invention, absent some teaching or suggestion supporting the combination." ACS Hos~. Sys., 732 F.2d at 1577,221 USPQ at 933. [837 F.2d at 1075,s USPQ 2d at 1599.1

The Court concluded its discussion of this issue by stating that teachings or references can be combined only if there is some suggestion or incentive to do so.

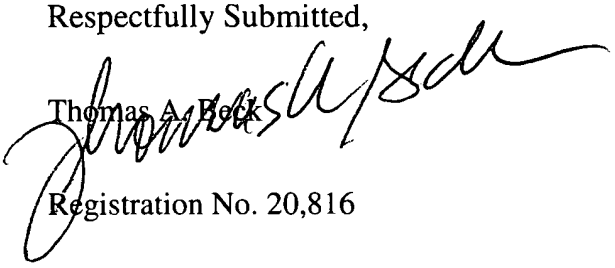
In the present case, the skilled artisan, viewing the references would not be directed toward Applicants' system. There can reasonably be no system such as Applicants emanating from the Tayloe and Findikli, et al. references as the basic focus of the two references are different. There is no proper basis to combine them.

Applicants have attempted in this response to include language limitations to specifically define the invention and to clear up any ambiguities that may have existed in the wording heretofore. Applicants believe that the amended claims are in a form which should result in their allowability. If there are additions which could result in the claims being allowed, Applicants' attorney would be pleased to speak with the Examiner by phone concerning such actbn at a mutually agreeable time and will cooperate in any way possible.

Please address all future correspondence in this application to the undersigned at:

15 Alameda Place, Mount Vernon, NY 10552

Respectfully Submitted,



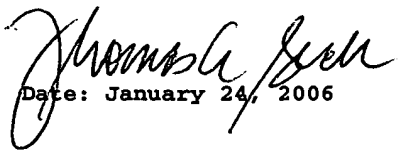
Thomas A. Beck

Registration No. 20,816

15 Alameda Place
Mount Vernon, NY 10552

(860) 921-1358

I hereby certify that this amendment response is being transmitted by the United States Postal Service, first class mail, postage prepaid, on the date indicated below addressed to Commissioner of Patents & Trademarks, Post Office Box 1450, Alexandria, VA 22313-1450



Date: January 24, 2006

APPENDIX A

1. (Currently Amended) A method for setting basic means of access for operation of devices of which the operation is controllable by electronic means, comprising: said devices comprising mobile phones, small computer-controlled consumer devices with relatively low level of computing power, computers, motor vehicles, control terminals for industrial processes, all of which devices may require authentication prior to operation, said authentication comprising a temporary deactivation which adds authorization patterns of progressive hierarchies of access rights to said devices prior to said operation ;

establishment of a non split-key link between a personal authentication system supplied with encryption data-and a logic system able to control an electronic device control, said encryption data being stored solely in said authentication system;

checking said encryption data in said authentication system prior to operation of said electronic device control;

assignment of a plurality of predetermined means of access to said electronic device control associated with said authentication system, said predetermined means providing access to physical hardware resources and access to different software functions, based on the privileges of the user who identified himself to the system, said software function evaluates a security token and is running on top of said physical hardware,

said predetermined means of access being dependent upon the level

of authorization that is set in said personal authorization system; enabling of said predetermined means for access for said authentication system dependent on the result of said check.

2. (Previously presented) The method defined in Claim 1, wherein said basic means of access to functions of said device comprise at least one of the following means: disable operation of said devices, enable operation of said devices, or enable configuration of said devices.

3.(Previously presented) The method defined in Claim 2 wherein said link is made without need for intermediate software layers.

4. (Previously presented) The method defined in Claim 3 includes in addition, the step of reading at least one of the following features embodied within said authentication system: firmware programs, device-specific command sequences for execution of specific device-specific functions, cryptographic keys, cryptographic algorithms, and individual decision-making logic.

5.(Previously presented) The method defined in claim 4 which includes configuration of said devices; by authorized persons, wherein after successful authentication, device-specific configuration data are downloaded into said devices from said authentication system in accordance with said authentication systems or over a network.

6. (Previously presented) A device comprising the elements defined in Claim 5 for execution setting basic means of access for operations.

7. (Previously presented) An authentication system, created for authentication of a person or a group of people, comprising the elements defined in Claim 5.

8.(Previously presented) The authentication system defined in Claim 7 which is implemented in the form of a Smartcard .

9.(Previously presented) A system for setting basic means of access for operation of devices of which the operation is controllable by electronic means, including at least one device and an authentication system as defined in Claim 8.

10.(Previously presented) A computer program, containing program code areas for the execution or preparation for execution of the steps of the method in accordance with Claim 4, when said program is installed in a computer.

11. (Currently Amended) A method for setting basic means of access for operation of devices of which the operation is controllable by electronic means, comprising: said devices comprising small computer-controlled consumer devices with relatively low level of computing power, computers, motor vehicles, control terminals for industrial processes, all of which devices may require authentication prior to operation said authentication comprising temporary deactivation which adds authorization patterns of progressive hierarchies of access rights to said devices prior to said operation; establishment of a non split-key link between a personal authentication system supplied with encryption data and a logic system able to control an electronic device control, said encryption data being stored solely in said authentication system; checking said encryption data in said authentication system prior to operation of said electronic device control;

assignment of a plurality of predetermined means of access to said electronic device control associated with said authentication system; said predetermined means providing access to physical hardware resources and access to

different software functions, based on the privileges of the user who identified himself to

the system, said software function evaluates a security token and is running on top of

said physical hardware, said predetermined means of access being dependent upon

the level of authorization that is set in said personal authorization system;
enabling of said means for access predetermined for said authentication system dependent on the result of said check.